Стремительное развитие телекоммуникационных технологий, роет числа электронных устройств и услуг, предоставляемых населению с использованием информационных технологий, привело к значительному увеличению количества киберпрестунлений. Появилось множество видов мошенничеств, направленных на получение конфиденциальных данных и дальнейшее их использование в корыстных целях. К числу одних из самых популярных из них можно отнести фишинг. Впервые понятие мошенничества под названием «фишинг» было использовано в 1996 году, когда злоумышленники, представляясь сотрудниками крупного

американского интернет-провайдера AOL, собирали идентификационную информацию пользователей (логины и пароли для входа в аккаунт). В результате от имени этих людей производились рассылки спама.

В дальнейшем обнаружилось, что таким способом можно получить не только доступ к аккаунту, но и к данным платежных карт, которые зачастую привязываются к личному кабинету. С развитием истории фишинга в начале XXI века пострадали платежные системы, а с 2005-2006 гг. - социальные сети, интернет-магазины, сайты крупных компаний.

Фишинг (англ, phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, цель которого — получить

идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации. Говоря простыми словами, фишинг - это кража информации в сети.

Какую же цель преследует фишинг и какого рода информация может понадобиться мошенникам?

Цели могут быть самые разные. Например:

1. Приватная информация частных лиц с целью их скомпрометировать. Хакеры могут охотиться как за известными личностями (например, с целью шантажа), гак и за обычными людьми.
2. Получение доступа к банковским счетам путем хищения логина и пароля от платежных сервисов.
3. Коммерческая тайна. Фишинг используется недобросовестными конкурентами, рейдерами (специалисты по смене собственников предприятия, действующие незаконными способами) и другими лицами, заинтересованными в получении доступа к ценной информации или к деньгам компании.

Фишинг используют, играя на чувствах и эмоциях, присущих большинству из пас. Это могут быть как отрицательные качества человеческой натуры: лень, жажда легких денег, любопытство и даже

ревность, так и абсолютно естественные чувства честного человека: страх - перед возможным банкротством или невозможностью погасить долг, боязнь быть обманутым и др.

Последние несколько лет атаки фишеров становятся все более продуманными, применяются методы социальной инженерии. Но в любом случае клиента пытаются напугать, придумать критичную причину для того, чтобы он выдал свою личную информацию. Как правило, сообщения содержат угрозы, например, заблокировать счет в случае невыполнения получателем требований, изложенных в сообщении («если вы не сообщите ваши данные в течение недели, ваш счет будет заблокирован»). Забавно, но часто в качестве причины, по которой пользователь якобы должен выдать конфиденциальную информацию, фишеры называют необходимость улучшить аптифишинговые системы («если хотите обезопасить себя от фишинга, пройдите но этой ссылке и введите свой логин и пароль»).

Следует отметить, что Фишинговые сайты, как правило, живут недолго (в среднем — 3-5 дней). Так как анти-фишинговые фильтры довольно быстро получают информацию о новых угрозах, фишерам приходится регистрировать все новые и новые сайты. Внешний же вид их остается неизменен — он совпадает с официальным сайтом, под который пытаются подделать свой сайт мошенники.

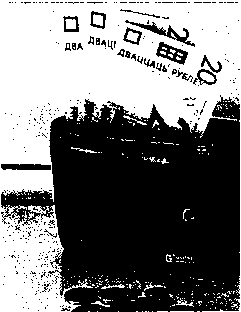
Зайдя на поддельный сайт, пользователь вводит в соответствующие строки свой логин и пароль, а далее аферисты получают доступ в лучшем случае к его почтовому ящику, в худшем — к электронному счету. Но не все фишеры сами обналичивают счета жертв. Дело в том, что обналичивание счетов сложно осуществить практически, к тому же человека, который занимается обналичиванием, легче засечь и привлечь мошенников к ответственности. Поэтому, добыв персональные данные, некоторые фишеры продают их другим мошенникам, у которых, в свою очередь, есть отработанные схемы снятия денег со счетов.

Наиболее частые жертвы фишинга — банки, электронные платежные системы, аукционы. То есть мошенников интересуют те персональные данные, которые дают доступ к деньгам. Но не только. Также популярна кража личных данных от электронной почты — эти данные могут пригодиться тем, кто рассылает вирусы или создает зомби- сети (ботнет).

Характерной особенностью фишинговых писем является очень высокое качество подделки. Адресат получает письмо с логотипами банка / сайта / провайдера, выглядящее в точности так же, как настоящее. Ничего не подозревающий пользователь переходит по ссылке наподобие

«Перейти на сайт и авторизоваться», но попадает на самом деле не на официальный сайт, а на фишерский его аналог, выполненный с высочайшей точностью.

Еще одной хитростью фишеров являются ссылки, очень похожие на URL оригинальных сайтов. Многие не помнят точный адрес сайта банка и ищут его через поисковые запросы. Поисковик выдает все подходящие страницы, и часто первые из них — как раз поддельные сайты банка, созданные мошенниками. Такой фишинговый сайт, как правило, повторяет дизайн официального сайта банка, но имеет другой интернет­адрес. На первое место в поисковой выдаче он попадает благодаря оплате рекламы, поэтому и обладает отличающейся от настоящего сайта пометкой «реклама». Из других признаков — зависание сайта после ввода реквизитов из-за «проведения технических работ». В общем, когда ничего не подозревающий клиент вводит свои логин и пароль на сайте, мошенники сразу получают доступ к счетам клиента. Что интересно, часто они не снимают деньги сразу, а выжидают, пока вы получите зарплату.

Не каждый пользователь может обратить внимание на то, что в командной строке браузера высвечивается ссылка, совершенно либо частично отличная от легитимного сайта. Такие «левые» ссылки тоже встречаются, но рассчитаны они на менее искушенного пользователя. Иногда они начинаются с IP-адреса, хотя известно, что настоящие солидные компании давно не используют подобные ссылки.

Также в самом теле письма может высвечиваться ссылка на легитимный сайт, но реальный URL, на который она ссылается, будет другим. Бдительность пользователя притупляется еще тем, что в письме может быть несколько второстепенных ссылок, ведущих на официальный сайт, но основная ссылка, по которой пользователю надо пройти и залогиниться, ведет па сайт мошенников.

Иногда личные данные предлагается ввести прямо в письме. Необходимо помнить, что никакой банк (либо другая организация, запрашивающая конфиденциальную информацию) не будет этого делать подобным образом.

Технологии фишеров не стоят на одном месте, постоянно видоизменяются и совершенствуются. Так, появилось сопряженное с фишингом понятие — фарминг. Это тоже мошенничество, ставящее целью получить персональные данные пользователей, но не через почту, а прямо через официальные веб-сайты. Фармеры заменяют на серверах DNSцифровые а/феса легитимных веб-сайтов на адреса поддельных, в результате чего пользователи перенаправляются на сайты мошенников. Этот вид мошенничества еще опасней, так как заметить подделку практически невозможно.

Наиболее популярные фишерские мишени — аукционы, торговые площадки, финансовые и платежные системы. Также страдают различные банки по всему миру. Атаки фишеров бывают случайными и целевыми. В первом случае атака производится «наобум». Атакуются наиболее крупные и популярные объекты — такие как торговые площадки — так как вероятность того, что случайный получатель имеет там учетную запись, довольно высока. Во втором случае мошенники узнают, каким именно банком, платежной системой, провайдером, сайтом пользуется адресат. Этот способ более сложен и затратен для фишеров, зато больше шансов, что жертва купится на провокацию.

К одной из основных причин успеха фишинг-афер следует отнести низкий уровень осведомленности пользователей о правилах работы компаний, от имени которых действуют преступники. И хотя на многих сайтах, требующих конфиденциальной информации, опубликованы специальные предупреждения о том, что они никогда не просят сообщать свои конфиденциальные данные в письмах, пользователи продолжают слать свои пароли мошенникам. Пока же основной защитой от фишинга остаются спам-фильтры и личная цифровая осведомленность граждан.

Вероятно, у многих граждан возникал вопрос - почему нельзя просто взять и заблокировать фишинговые сайты?

Во-первых, они растут как грибы после дождя, и уследить за ними физически сложно. Во-вторых, хотя фишинговые сайты — нарушение закона «О рекламе», чаще всего они созданы не в Беларуси, и устрашать мошенников нашим законодательством и ответственностью бесполезно.

Советы, как не стать жертвой фишера.

Для того, чтобы не стать жертвой киберпреступников, совершая сделки в сети Интерпег следует:

* вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы);
* ведя общение с пользователем стоит перейти к его профилю и обратить внимание па дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);
* очень внимательно относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга). Самый надежный способ уберечь свои средства - это никому не сообщать реквизиты своей карты;
* для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы, обязательно проверяя доменное имя ресурса в адресной строке браузера;
* следует воздерживаться от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги, благотворительной и спонсорской помощи в пользу организаций и физических лиц при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают;
* уточнить у собеседника номер телефона если он не указан в объявлении, а потом позвоните на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку (очень часто злоумышленники используют номера телефонов, взятые в аренду на непродолжительное время и физического доступа к нему, не имеют);
* избегать перехода по неизвестным иигернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки. Если Вам прислали такую ссылку, то, независимо от того, кто ее прислал, прежде чем по ней перейти, следует внимательно проверить доменное имя (адрес ресурса). Сделать это можно отыскав в интернете официальный сайт и сверив написание доменного имени. Отличие в одну букву или символ свидетельствует о том, что перед Вами ссылка на поддельный ресурс.
* необходимо использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему; установить антивирусную программу не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

Если вы уже пострадали от фишинга: отправили кому-то данные банковской карты, включая CVV-код, или пароль от платежной системы - немедленно обратитесь в банк, а в случае необходимости - в правоохранительные органы.